ON CYBER

THE GRUGQ
@THEGRUGQ

IVE BEEN IN THIS
GAME FOR YEARS

HACKING IN THE 90S

```
10 FIND 0DAY
20 HACK THE PLANET
30 GOTO 10
```

THE GAME

citigroup

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

KASPERSKY lab

eEye Digital Security®

THE GAME: CYBERSECURITY 2000

- Cleanup after breaches
  - Usually by script kiddies w/ egg drops
- Clean up malware
  - Sometimes by cybercriminals
- Coordinate vulnerability disclosure
  - (At least this one has been solved)

THEN, ONE DAY...

THE GAME GOT WEIRD

THE GAME GOT BIG

THE GREAT GAME

APT

ALSO APT

BEST APT

INEVITABLE

INFORMATION WANTS TO BE FREED

THE NEW NORMAL

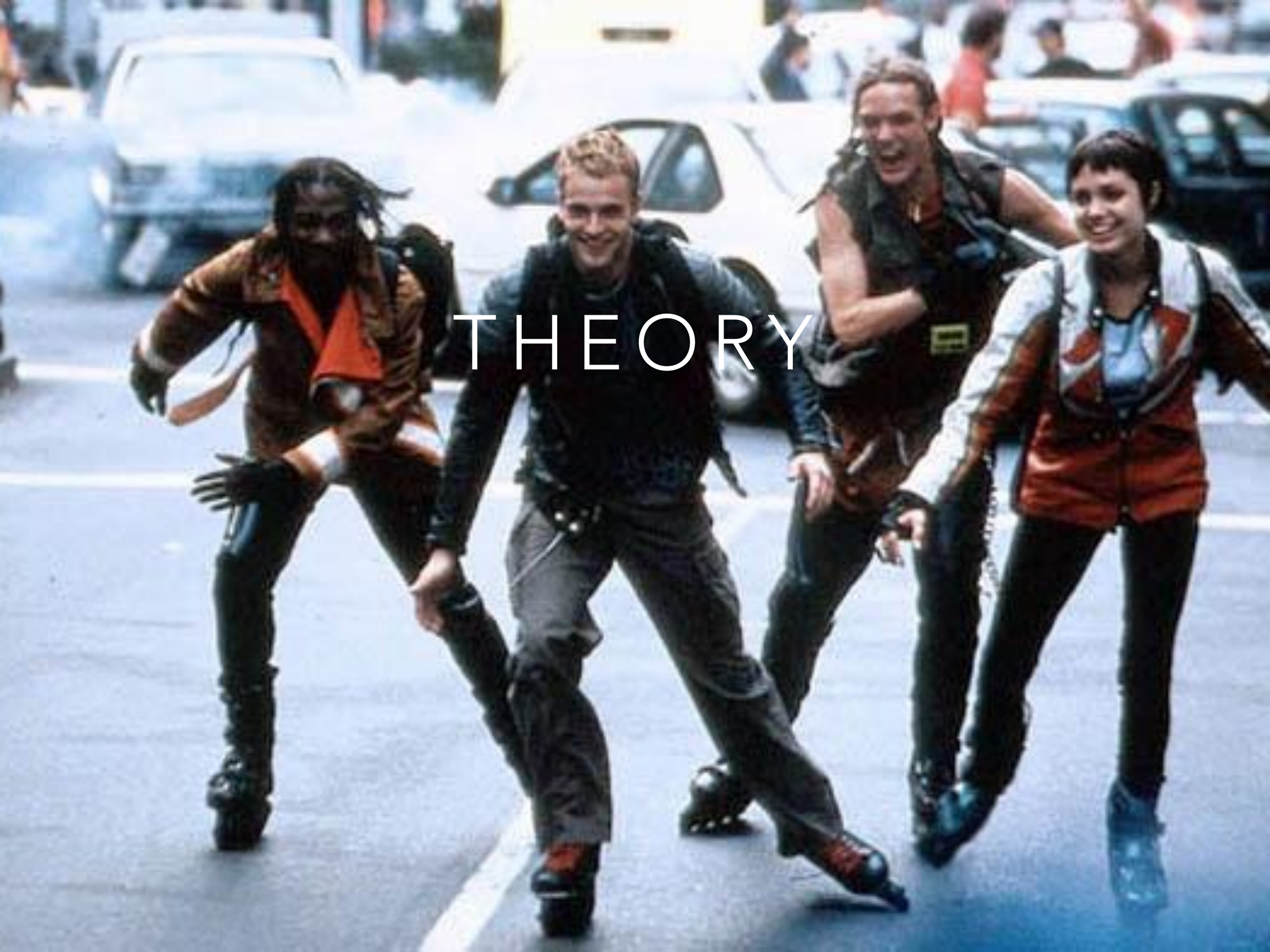
WE’RE HERE

NOW WHAT?

THE GREAT CYBER GAME

CYBERWAR

THEORY



REALITY

WELL THAT SUCKS

WHY SO VERY WRONG?

NEW DOMAINS OF CONFLICT

ARE INFREQUENT

HARD TO PREDICT

THEORY MEETS PRAXIS

THIS HAS HAPPENED

BEFORE

AN ANALOGY

A NEW DOMAIN OF CONFLICT

AIR POWER 1915

AIR POWER 1915: TECHNOLOGY

- Airplanes were basically motorised kites
- No weapons
- Used for reconnaissance
    - Critical to accurate artillery fire

AIR POWER: TACTICAL THEORY

- Highly skilled pilots
  - Highly manoeuvrable planes
    - Battle for supremacy in bouts of skill and daring!
- Takeaway
  - Build highly manoeuvrable planes

PRACTICE...

AIR POWER 1917: EXPERIENCE

- Practical rules for air war
  - Boelke Dicta
  - Similar rules from Western aces
- Proven in the crucible
- Concerned only with winning, not chivalry
- Takeaway
  - Fast planes that can climb high

DICTA BOELKE

- Secure the upper hand before attacking
- Always continue an attack you have begun
- Only fire at close range, when target is in sights
- Always keep an eye on your opponent

DICTA BOELKE CONT.

- In any attack, attack from behind
- If opponent dives on you, turn to meet the attack
- When over enemy lines, never forget line of retreat
- Attack in groups

“There are two types of planes: fighters, and targets”

AIR FORCE SAYING

FIGHTER

TARGET

OVERWHELM THE WEAK

GO IN QUICK

HIT HARD

GET OUT

TACTICAL CYBER

CYBERWAR 2015: IN THEORY...

CYBER CONFLICT 2015: PRACTICE

- Experience has produced some basic rules about winning
- Hit the softest targets the hardest

TARGETED ATTACK DEMO

QUANTUM

- Why does NSA hit browsers?
  - Targeted
  - Easy*
  - It works

APT

- Why does Asia Pacific Threat do spear phishing?
  - Targeted
  - Easy
  - It works

EVERYONE

- Why do all* nation states use phishing?
  - Targeted
  - Easy
  - It works

WHAT WORKS

- Client sides
  - Spear/phishing
  - Browsers
- USB
- Web Apps
- Other:
  - Interdiction, telnet sniffing, big boy stuff…

CYBER TACTICS

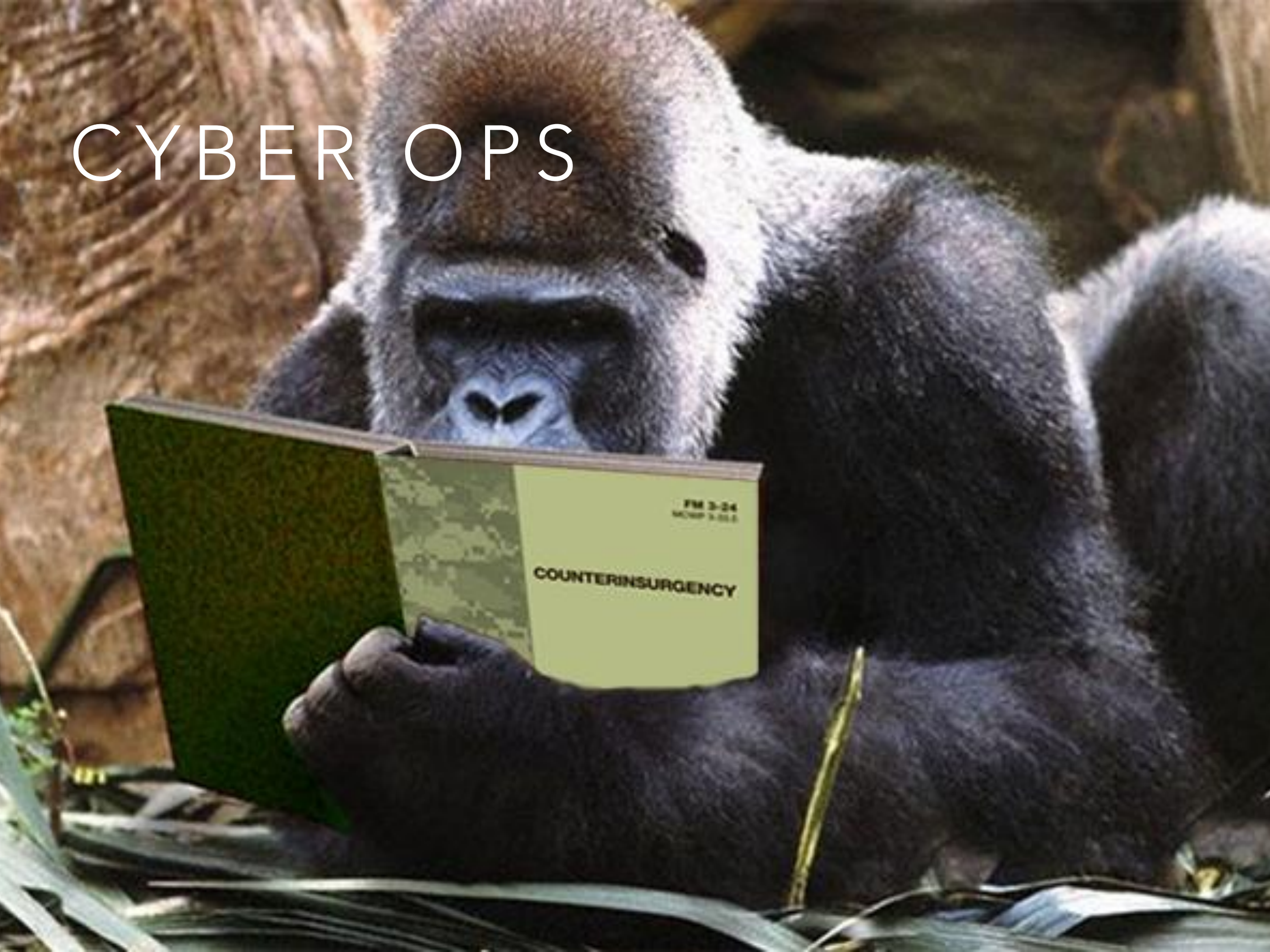
OVERWHELM THE WEAK

GO IN QUICKLY

HIT HARD

GET OUT

CYBER OPS



OPERATION PHASES

- planning
- preparation
- execution
- finish

SPEC OPS

- simplicity
- security
- repetition
- surprise
- speed
- purpose

CYBERWAR 2015

ADVERSARIAL ORGANISATIONS

CHINA

RUSSIA

INDIA


"Non-Violence is the greatest force at the disposal of Mankind.
It is the supreme law. By it alone can mankind be saved."
-Mahatma Gandhi
MOHANDAS K. GANDHI
October 2, 1869 - January 30, 1948
"My Life is My Message"

NORTH KOREA

TOOLCHAINS

- An investment and an expense
  - Constant maintenance
- Tools, Techniques & Procedures are Commitments

STRATEGIC CYBER

"data packets are like bullets and your walls of fire are like the armor that repels them."

–TWO STAR GENERAL, CYBER COMMAND

THE TECHNICAL MEANS OF WARFARE

AERONAUTICS OPENED up to men a new field of action, the field of the air. In so doing it of necessity created a new battlefield; for wherever two men meet, conflict is inevitable. In actual fact, aeronautics was widely employed in warfare long before any civilian use was made of it.[7] Still in its infancy at the outbreak of the World War, this new science received then a powerful impetus to military development.

The practical use of the air arm was at first only vaguely understood. This new arm had sprung suddenly into the field of war; and its characteristics, radically different from those of any other arm employed up to that time, were still undefined. Very few possibilities of this new instrument of war were recognized when it first appeared. Many people took the extreme position that it was impossible to fight in the air; others admitted only that it might prove a useful auxiliary to already existing means of war.

WHAT CAN HELP?

"PREPARE
TO MEET THY
GOD"

MANOR ST.

SECURITY VENDORS' SOLUTIONS

YOU WILL BE DISAPPOINT

STUNT HACKING

INFOSEC INDUSTRY

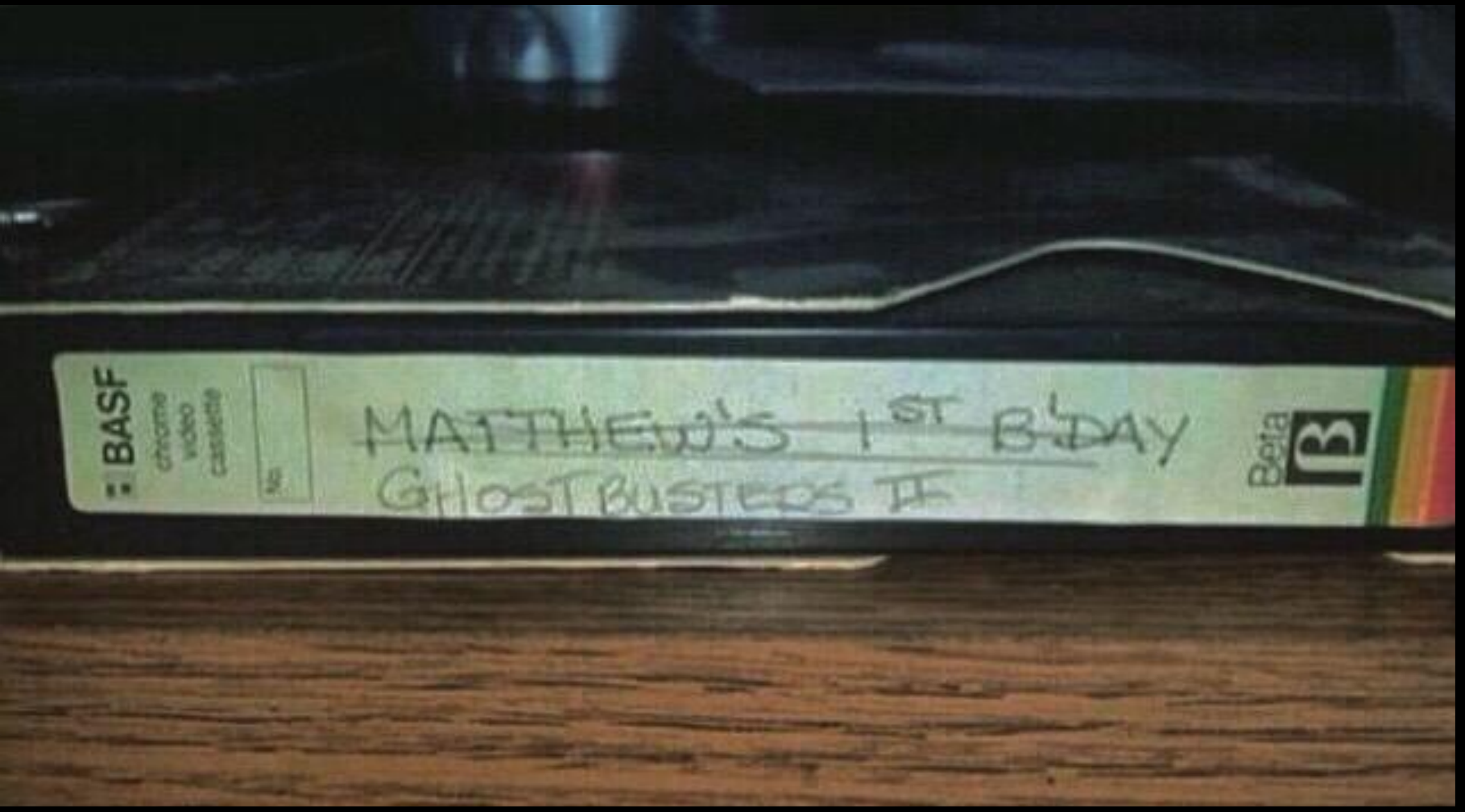
DISASTER TOURISTS

CISSP

GOOD LUCK WITH THAT

NATIONAL INTELLIGENCE AGENCIES

DON'T LOVE YOU




THREAT
"INTELLIGENCE"
memegenerator.net


IT WAS
CHINA
imgflip.com

WHAT WORKS

EARLY DETECTION

COMPARTMENTATION

TIME IS ON YOUR SIDE


POLICE
YC13 MFN

ENJOY THE VIEW

THANK YOU